IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH

IN THE MATTER OF THE SEARCH OF AN IPHONE 13 PRO S/N W4VXVX67C9 SEIZED FROM JESSE HARTWELL ON MAY 19TH, 2023, CURRENTLY LOCATED AT THE HSI FORENSIC LAB IN WEST VALLEY CITY	Case No. 2:23mj513 JCB

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Special Agent (SA) Holden Fielding, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed with Homeland Security Investigations as a Special Agent since September 13th, 2020. I have a degree in criminology from the University of Utah, which I completed in July of 2020. This degree included taking classes regarding gangs and gang violence, family violence and exploitation, and cyber security. I attended and graduated from the three month long Criminal Investigator Training Program at the Federal Law Enforcement Training Center in June of 2021, and the Homeland Security Investigations Special Agent Training program in September of 2021 at the Federal Law Enforcement Training Center in Glynco, GA. These programs come to a total of 1011 training hours, which included training specific to Child Exploitation. As a federal agent,

I am authorized to investigate violations of laws of the United States and is a law enforcement officer with the authority to execute warrants issued under the authority of the United States. I have also received training specific to undercover chatting in relation to child exploitation from the Internet Crimes Against Children Task Force (ICAC) and is certified as an Undercover Chatter.

PURPOSE OF THE AFFIDAVIT

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of a cellular telephone (the "SUBJECT DEVICE," described in Attachment A,) for the fruits, evidence and instrumentalities of violations of 18 USC § 2422 (b), Coercion and Enticement for Illegal Sexual Activity; 18 USC § 2252A(a)(2) Receipt/Attempted Receipt of Child Pornography; and/or 18 USC § 2252A(a)(5)(B) Possession/Attempted Possession of Child Pornography (the "SUBJECT OFFENSES"), as described in Attachment B.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

BRIEF SUMMARY

4. As set forth in detail below, in May, 2023, I was posing undercover online as a man who was molesting his five-year-old son when I was contacted by Jesse Hartwell ("HARTWELL"). On May 19th, 2023, HARTWELL arranged to meet in order to molest the child himself. During the chat, HARTWELL graphically described the sex acts he intended to perform on the child including oral sex and anal rape. During these chats, HARTWELL also discussed child pornography that he possessed, describing videos that included the violent rape of children. He indicated that he would be bringing the child pornography with him. When HARTWELL

arrived at the meeting, he was arrested in possession of a cellular telephone - the SUBJECT DEVICE. There is probable cause to believe that the SUBJECT DEVICE was used by Hartwell to communicate with me about the SUBJECT OFFENSES, and is fully capable of taking, downloading, and storing child pornography. Thus, there is probable cause to believe that the SUBJECT DEVICE contains fruits, evidence, and instrumentalities of the SUBJECT OFFENSE. The cellular telephone was seized pursuant to arrest but has not been searched.

PROBABLE CAUSE

5. In May, 2023, I posed online undercover on a social media application as an individual interested in "taboo." I was contacted by an individual later identified as Jesse HARTWELL. While HARTWELL's username on the social media application was "Erik," the photos attached to his profile depicted HARTWELL's face. After chatting briefly on the social media application, I suggested that we move our conversation to a chatting application and sent him the username for my undercover chat account.

6. Shortly thereafter I received a message from HARTWELL on my undercover chat account. In his initial message, HARTWELL confirmed that he was "Erik" from the previous social media application. Almost immediately HARTWELL told me that he was into "young, dad/son, man/boy stuff here, and more." At that point I informed HARTWELL that I "play" with my five-year-old son. In this context I meant that I was molesting my son. HARTWELL clearly understood this because he responded "fuck!!! Do you fuck him? How long you been playing with him?" He also said "that's fucking hot man. Hell yea. Does he cry and scream? My favorite ages are 2-7 but I don't care how old they are. Biggest fantasy is to pound a 2 y.o. I want one so bad."

7. After HARTWELL told me that he wanted to molest a child, I told him that I enjoyed watching other men molest my son. HARTWELL then responded by saying "i would be down for that man. seriously."

8. Over the next few hours, HARTWELL graphically described the sex acts he wanted to perform on the child, including oral and anal sex.

9. HARTWELL also made it clear that he wanted to perform sadistic acts on the child, making him cry and scream in fear, humiliation, and pain. HARTWELL asked if I had any rules about what he could, and could not, do to the child, because, he said, "I have a sadistic streak lol." I told him that the only rule was not to leave any marks on the child that daycare could find. Defendant replied "no marks? That's easy!" Later on, HARTWELL reiterated "so … as long as there are no marks on him you're good right? like if I had him crying and maybe even screaming it's all good? Just making sure." Later, he reiterated "I love that you don't mind if he cries or feels pain. that is so awesome to me. He's basically a sex slave." HARTWELL also said he wanted to make the child sit on his lap while he scares him with details of what is going to happen, degrade him, spank him, spit on him, make him "choke on my dick" and "choke him a little.

10. HARTWELL also graphically expressed his intent to ejaculate in the boy's mouth and anus.

11. During our chat, HARTWELL said he "collects." Based on my training and experience, "collecting" in this context is common vernacular for collecting child sex abuse material (commonly referred to as child pornography). HARTWELL graphically described a number of the videos he viewed. For example:

a. "one video that really gets me off. The poor little slut is bent over on the edge of the bed and their arms and legs are tied down spread eagle… can't move. Blindfolded. I love guys that are just relentless. Even if the kid is too tight. They don't let that stop them. It's going in. lol."

b. "there's one video I saw a while back that I can't find… two dads, gay couple with a boy, one in his ass and the other is in his mouth, and they're doing him hard, the boy can't take it. Was one of the hottest things I've seen when husbands have fun with their boy."

c. HARTWELL asked if I was familiar with a particular person who is known to have molested his younger brother and produced child pornography of him. HARTWELL indicated, "the little bro is so cute. Reddish blonde hair, innocent face. And [the adult] just shoves his big dick in him like it's nothing. Love hearing him moan. And when he cu[m]s… oooof. The boy can't be but a little over a year old either. Can't talk or anything. Can't say no or fight back. Just has to take it! That's what I like to see."

12. During the chat, HARTWELL claimed that he had previously molested a 2-year-old girl along with her father, and knew other individuals who were molesting their children. He claimed that he had never produced child pornography himself, but wanted to.

13. HARTWELL and I arranged to meet in person on May 19th, 2023, so that HARTWELL could molest my 5-year-old son. He informed me that he would be taking an Uber to the prearranged location and would let me know when he was there, so I could meet him in the parking lot. HARTWELL arrived at the pre-arranged location as the passenger in

a car and was dropped off; he was then arrested. The SUBJECT DEVICE was in his possession at the time and seized pursuant to his arrest.

14. HARTWELL's appearance matches the profile picture of the social media account of "Erik," the person with whom I had been communicating. Post-Miranda, HARTWELL admitted that he had been communicating with a man who had a five-year-old child and had discussed molesting the five-year-old boy himself.

15. The SUBJECT DEVICE was the only electronic device in HARTWELL's possession at the time of his arrest, so it would have to be the device HARTWELL would have used to let me know he had arrived at the location. Further, it is capable of supporting the social media and chat applications used to communicate with my undercover persona about the rape of children. Therefore, there is probable cause to believe that there will be evidence on the SUBJECT DEVICE of our communications and evidence that HARTWELL is the true identity of "Erik," with whom I had been communication.

16. Further, during the chats HARTWELL expressed a sexual interest in children and sexual images of children. I know from training and experience that individuals like HARTWELL who have a sexual interest in children often use electronic devices to access, download, share, produce, and retain child sexual assault material (CSAM) or child pornography for continued viewing. Electronic devices like the one seized from HARTWELL allow sex offenders to store evidence of their crimes against children and evidence of crimes against children committed, recorded and shared by other sex offenders. Such devices can also be used to access, share, and copy such material from remote servers, directly from the devices of other pedophiles or from other devices accessible to the user such as their desk top computers, lap top computers or other electronic devices. Given that HARTWELL told me that he collects CSAM and

described various videos of CSAM in the chat, I believe it is reasonable to assume that evidence of crimes against children may at this time be stored on his device.

17. The SUBJECT DEVICE is currently located in evidence at the HSI forensic lab, located at 2975 Decker Lake Drive West Valley City Utah 84119. It has not been searched. In my training and experience, I know that the SUBJECT DEVICE has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the SUBJECT DEVICE first came into the possession of HSI.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

18. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

19. There is probable cause to believe that things that were once stored on the SUBJECT DEVICE may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not

actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives or internal memory storage—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files.

d. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

20. HARTWELL used a social media application to communicate with me. Based on my training and experience, some social media applications require payment. He further disclosed to that he collects child pornography; unless he produced those images, he had to obtain these images from someplace; based on my training and experience some child pornography is available

for free via the Internet but some child pornography requires payment. Financial records stored on the phone may establish who was in possession of and using SUBJECT DEVICE when the listed offenses were committed, may help identify victims, may reveal payments made by HARTWELL for social media applications in which he communicated with the undercover agent (me) or others regarding his sexual interest in children, or payments made by HARTWELL in exchange for child pornography, and may reveal his purchase of or use of applications to facilitate the listed crimes which have since been deleted. Through my training and experience I have learned internet applications ("apps") can be downloaded, used, and deleted after use to conceal or destroy evidence of criminal conduct that includes text messages and picture and video files. Many "free" apps require the user to provide financial information such as credit card, debit card or bank account information. Many apps solicit subsequent "in app" purchases which are made with the financial card or account information provided when the user registered the account. Other apps require an actual up front purchase expense. Financial records can provide documentation of which apps the user downloaded or purchased, when the device user used the SUBJECT DEVICE to download apps, or buy more data or telephone call minutes, even after the apps and related accounts have been deleted by the user.

21. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the SUBJECT DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage

medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage Devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a Device can also indicate who has used or controlled the Device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an adult individual like HARTWELL uses an electronic device to hunt for child victims to sexually exploit and assault the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense. In cases like the one described herein, the device may also contain and is likely to contain information which may assist in identifying and protecting child victims of sexual exploitation.

22. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the SUBJECT DEVICE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to use of the password provided by HARTWELL and/or computer- assisted scans of the entire medium, that might expose many parts of the SUBJECT DEVICE to human inspection in order to determine whether it is evidence described by the warrant.

23. *Manner of execution.* Because this warrant seeks only permission to examine a

device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Respectfully submitted,

/s/ *Holden Fielding*
Special Agent
Homeland Security Investigations

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 on May 26, 2023:

JARED C. BENNETT
United States Magistrate Judge

ATTACHMENT A

The property to be searched (the "SUBJECT DEVICE") is an iPhone 13 Pro with a Serial Number W4VXVX67C9 seized from Jesse HARTWELL subject to his arrest on May 19th, 2023, in West Valley City, Utah and currently located in evidence at the HSI forensic lab, located at 2975 Decker Lake Drive West Valley City Utah 84119.

.

ATTACHMENT B

ITEMS/INFORMATION TO BE SEIZED

The items/information to be seized, which constitute fruits, evidence, and instrumentalities of 18 USC § 2422 (b), Coercion and Enticement for Illegal Sexual Activity; 18 USC § 2252A(a)(2) Receipt/Attempted Receipt of Child Pornography; and/or 18 USC § 2252A(a)(5)(B) Possession/Attempted Possession of Child Pornography (the "SUBJECT OFFENSES") are:

1. The SUBJECT DEVICE itself if its contents evidence that it was an instrumentality of the "SUBJECT OFFENSES".

2. All records on the SUBJECT DEVICE that relate to violations of the SUBJECT OFFENSES, including:

   a. Contents and data stored in or in connection with the social media application used to communication with the undercover agent in this case (this social media application is not identified herein but is known to law enforcement and will be provided to any individual executing the search of the SUBJECT DEVICE);

   b. Any and all records, documents, visual depictions, text messages, chat, and or other materials in any form related to any account associated with the username "Erik";

   c. Images, correspondence, and other records that tend to indicate the true identity of the individual with the username "Erik";

d. Any and all records, documents, visual depictions, text messages, chat, and or other materials in any form related to communications with the undercover agent in this case;

e. Any and all records, documents, visual depictions, text messages, chat, and or other materials in any form pertaining to child pornography, child erotica, an interest in such materials, or pertaining to a sexual interest in children, or sexual activity involving children;

f. Any and all records, documents, visual depictions, text messages, chat, and or other materials in any form pertaining to any minor who is, or appears to be, the subject of any visual depiction of child pornography, child erotica, sexual activity with other minors or adults, or of sexual interest, or that tends to identify any such minors, including but not limited to any biographical information, screen names, monikers, handles, user names, passwords, account names, email addresses or account information;

g. Any and all records, documents, visual depictions, text messages, chat, and or other materials in any form that reflects interest in sexual activity with children and the crime under investigation;

h. Any and all records, documents, visual depictions, text messages, chat, and or other materials in any form that reflect a sexual interest in or the sexual exploitation of minors or that help identify persons possessing, receiving, distributing or producing child pornography or the crime under investigation;

i. Location information associated with the SUBJECT DEVICE that is relevant to the crime under investigation that helps identify the user of the SUBJECT DEVICE or events relating to the crime to determine the chronological and geographic context of account access, use, and events relating to the crime and to the SUBJECT DEVICE's owner and the owner's contacts that are evidence of the crime under investigation;

j. Location information associated with the SUBJECT DEVICE that may help identify suspects, the account user, or show where events occurred, and who sent, received, possessed or produced child pornography or other evidence of the crime under investigation;

k. Any and all records, documents, visual depictions, text messages, chat, and or other materials in any form that tends to identify who may have participated in the crime under investigation;

l. EXIF or other metadata about images, documents or correspondence reflecting a sexual interest in children, or that help identify the device or person who produced, sent, traded, received, or possessed child pornography or that identifies the user of the SUBJECT DEVICE used to engage in child exploitative acts.

m. Any and all records, documents, visual depictions, text messages, chat, and or other materials in any form concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members, and/or that advertise, promote, discuss or otherwise involve child pornography;

n. Any and all records, documents, visual depictions, text messages, chat, and or other materials in any form membership in online groups, clubs, or services that discuss or otherwise involve the crimes under investigation;

o. Evidence indicating how and when the SUBJECT DEVICE was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation;

p. Evidence indicating the SUBJECT DEVICE's user's state of mind as it relates to the crime under investigation;

q. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts;

r. Records relating to who created, used, or communicated with the SUBJECT DEVICE's user, including records about their identities and whereabouts.

s. Contact lists.

t. Media files such as pictures, photographs, videos or screen shots.

u. any information recording HARTWELL's location or travel as he used the device and indicating the location of any potential child victims whom HARTWELL contacted or attempted to contact.

v. all bank records, checks, credit card bills, account information, and other financial records which indicate how he may have used SUBJECT DEVICE to facilitate violation of the listed crimes, to include enticing minors directly or indirectly to

create or send child pornography, or which indicate the user of the SUBJECT DEVICE'S location when he violated the listed crimes, to include attempts, or which document application/app purchases or in-app purchases which relate to apps which could be used to facilitate the sexual exploitation of children. My training and experience has taught me that apps can be deleted from electronic devices so that other means such as financial records may be the only evidence that the suspect once possessed or used the app.

3. Evidence of user attribution showing who used or owned the SUBJECT DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

4. Records evidencing the SUBJECT DEVICE connecting to the internet or to Internet Protocol addresses including:

a. records of Internet Protocol addresses used;

b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

5. Definitions:

a. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any

photographic form.

b. "Child Pornography" as used herein is defined in 18 U.S.C. § 2256(8). (Any visual depiction, including any photograph, film, video, picture, or computer or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

c. "Visual depictions" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

d. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions; this also includes texts or discussions regarding minors engaged in sexual acts or conduct.

6. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be

conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, law enforcement may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.